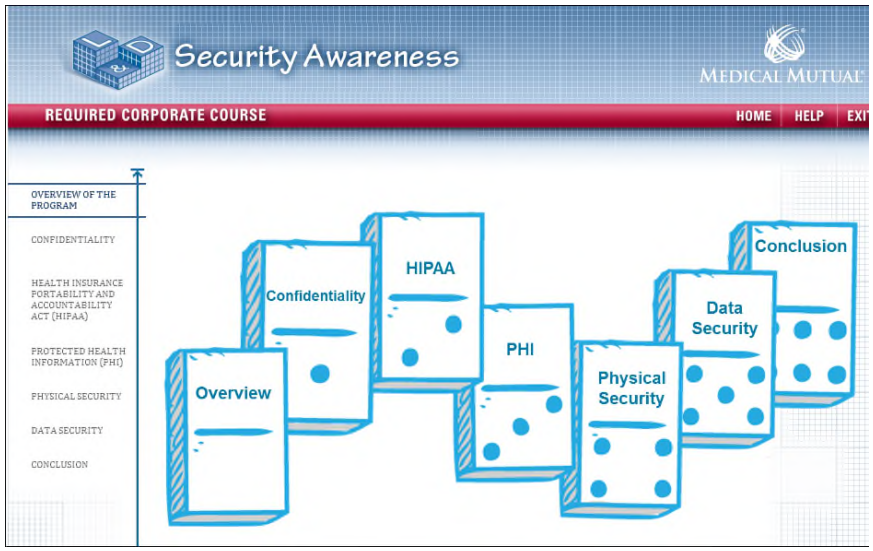
Medical Mutual Privacy and Information Security Awareness Training Program

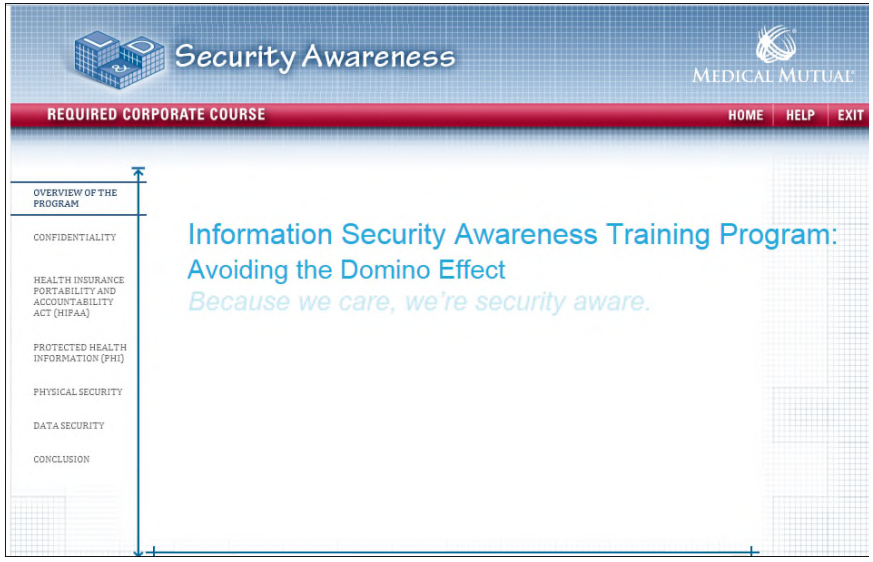
Avoiding the Domino Effect

Because we care, we're security aware.

This document is intended for those Medical Mutual employees and contract staff who do not have online access to this mandatory training module. Receipt of this document implies agreement and adherence to its contents.

Should the reader have questions or concerns regarding the document contents, please discuss with your direct Management and/or Enterprise Security,





Information Security Awareness Training Program: Avoiding the Domino Effect.

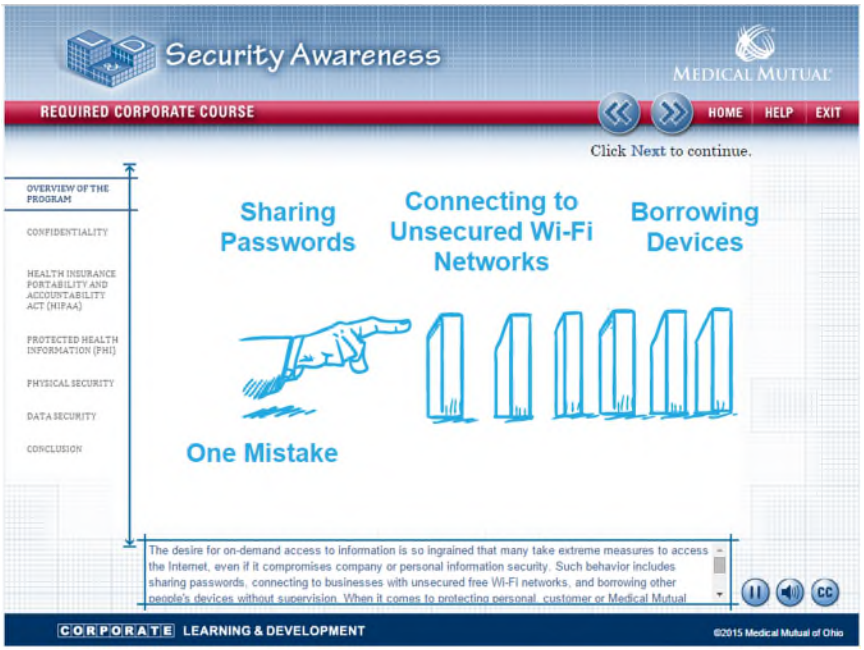
Because we care, we're security aware.

This module provides a brief overview of Medical Mutual Services' Information Security corporate policies and recommended best practices. You should contact your supervisor if you have any questions regarding these policies or if a situation arises that is not covered in the module.

Welcome to the Information Security Awareness Training Program. Confidentiality and privacy are the foundation of all data security. All employees must be mindful of their everyday activities in the workplace. Even the smallest mistakes can add up to a disaster.

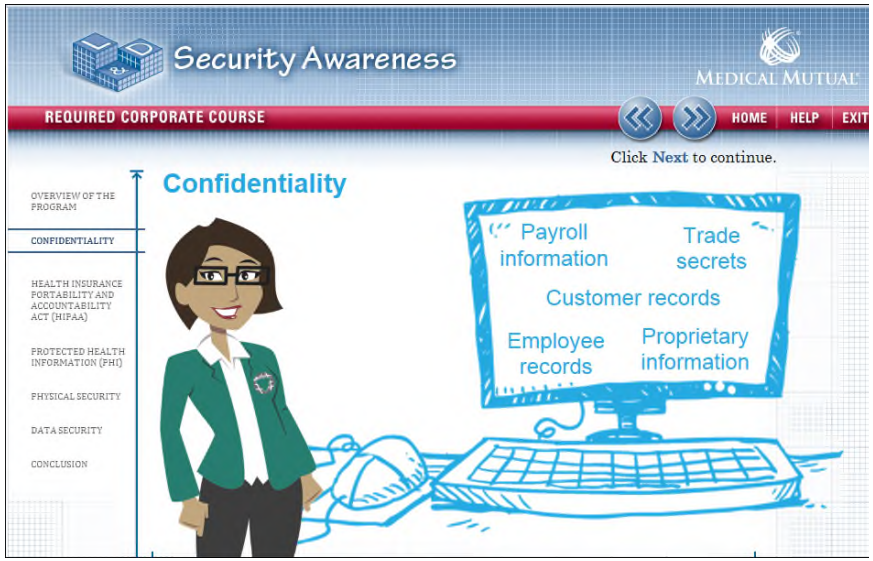
Throughout this module, Medical Mutual reminds you of the policies established to ensure data security. As an employee, you are provided with access to materials and resources to do your job. This includes access to sensitive data that has to be handled in a secure manner to ensure that Medical Mutual maintains its data security. Medical Mutual trusts that you will take this responsibility seriously and is providing this training to help you do so.

Throughout this training you'll be quizzed on how to follow the rules established by Medical Mutual.

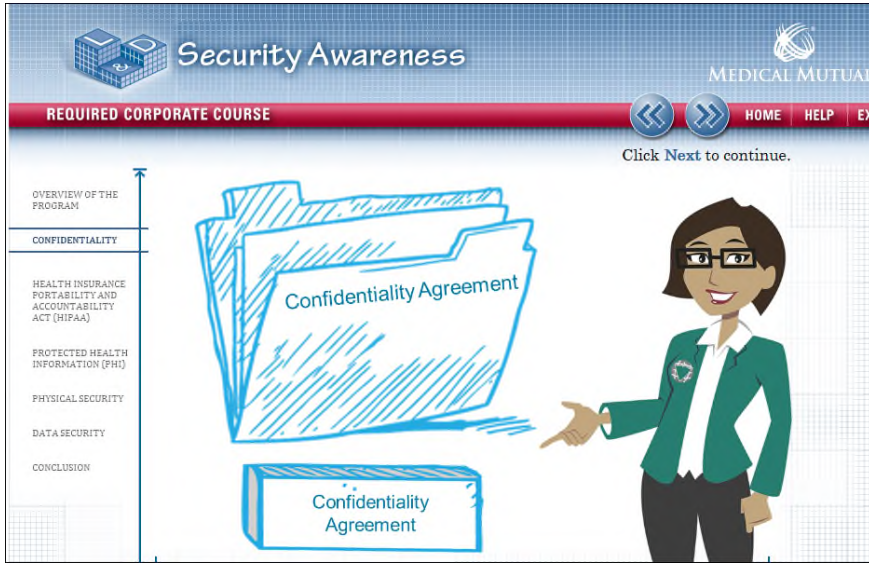


The desire for on-demand access to information is so ingrained that many take extreme measures to access the Internet, even if it compromises company or personal information security. Such behavior includes sharing passwords, connecting to businesses with unsecured free Wi-Fi networks, and borrowing other people's devices without supervision.

When it comes to protecting personal, customer or Medical Mutual data, no amount of technology or additional safeguards can substitute for conscientious employee behavior. The human factor plays a major role in security violations. All it takes is one little nudge and things can topple out of control.



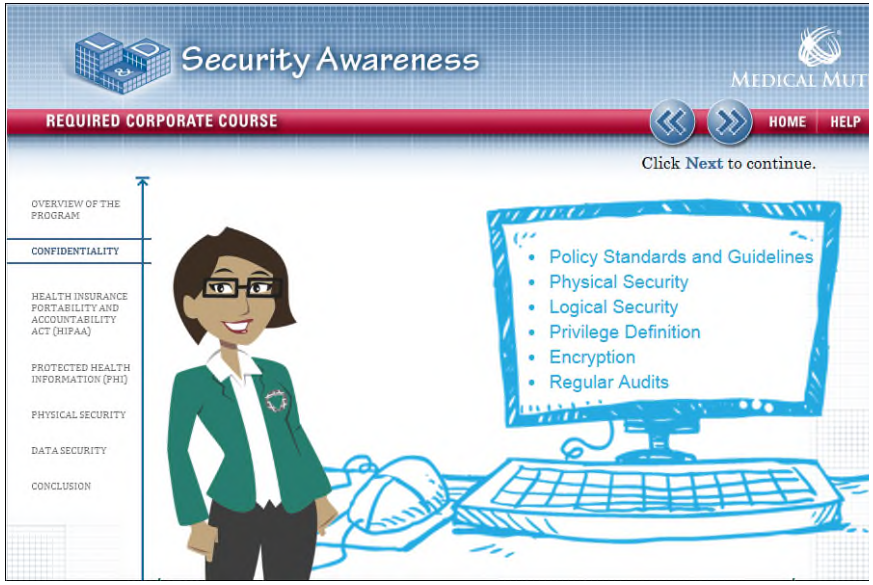
Data breaches affect individuals and companies: that means our customers, our employees and Medical Mutual. The information we store electronically includes not only customer records, but also employee records, trade secrets, payroll information and other Company proprietary information.



Medical Mutual employees have access to a variety of sensitive and confidential information.

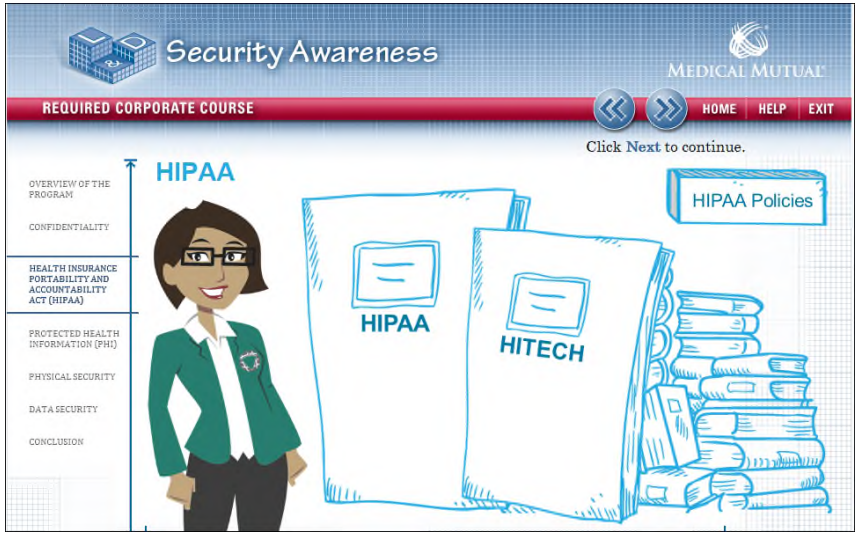
As a condition of your employment, you must agree to abide by the terms and conditions within the Company's Confidentiality Agreement. We also require such agreements from our contracted vendors, affiliates and other representatives.

By doing your part, you are helping to protect the information of Medical Mutual, its employees and customers.



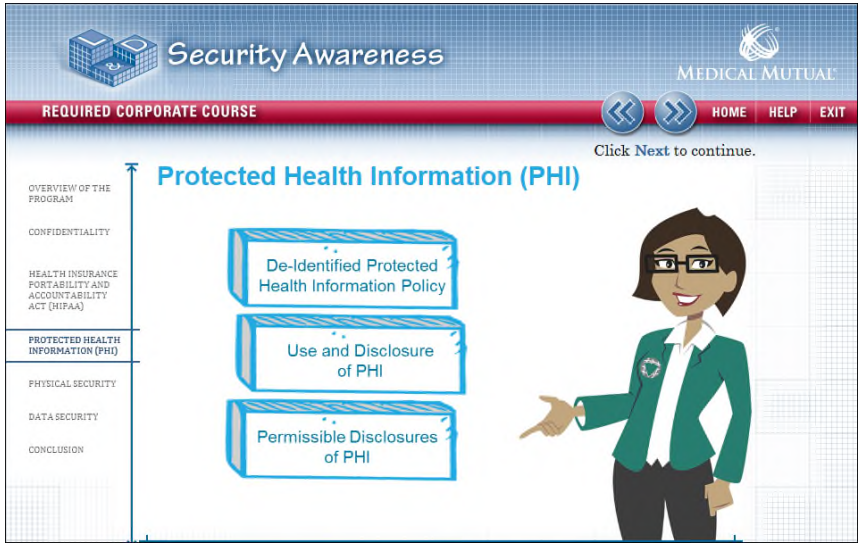
At Medical Mutual, we have a number of safeguards in place:

- Policy Standards and Guidelines, which set the basis for control related to data security, confidentiality, corporate communications, email, privacy, compliance with laws, acquisitions and conflicts of interest;
- Physical Security, such as key card access to Company offices and computing resources, and keeping a close eye on our buildings and grounds;
- Logical Security, including effective user account and password management;
- Privilege Definition, which includes the rules for employees' access and security rights;
- Encryption, which means translating data into a secret code. To read the data, you need a key or password; and Regular Audits.



The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), together with the related federal regulations and official guidance, govern the use and disclosure of Protected Health Information (PHI).

All employees need to understand the basics of HIPAA and HITECH as they relate to our business operations. Use and/or disclosure of Protected Health Information in violation of HIPAA/HITECH may subject Medical Mutual to civil penalties of up to $50,000 per incident and up to $1,500,000 for all violations of an identical provision and can result in fines and/or criminal charges against the company and/or employee.



PHI is information that relates to the past, present or future physical or mental health or condition of an individual that identifies the individual or can be used to identify the individual. The list of PHI identifiers is included in the "*De-Identified Protected Health Information Policy*."

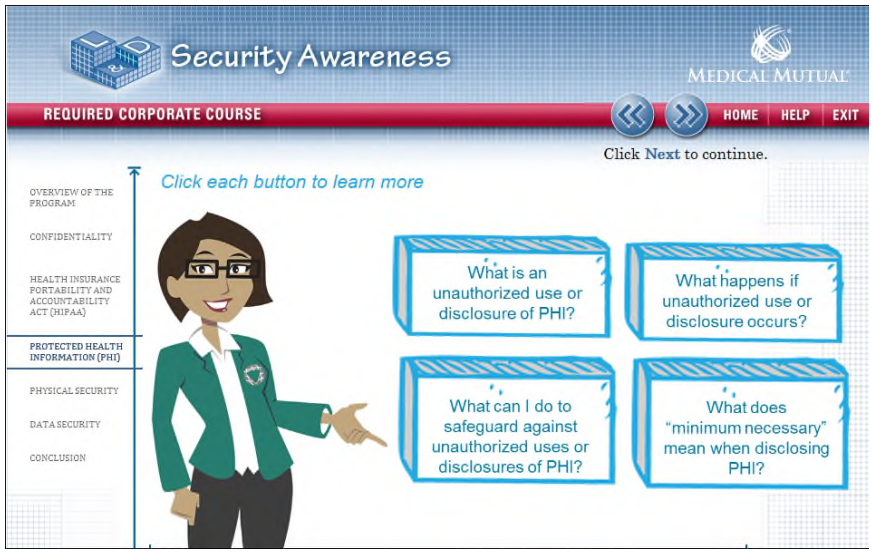
Use and Disclosure of PHI

Only under certain circumstances is PHI permitted to be used or disclosed. Generally, PHI can be disclosed:

1. To the person who is the subject of the PHI
2. To conduct certain treatment, payment or health care operations specified in HIPAA/HITECH
3. When authorized by the person who is the subject of the PHI, which authorization must meet certain requirements specified in HIPAA/HITECH
4. When we are required by law to release it
5. To a vendor or subcontractor who has signed a business associate agreement with us
6. To groups under certain conditions specified in HIPAA/HITECH
7. When all identifying information is removed in accordance with HIPAA/HITECH

Also, when a use or disclosure of PHI is permitted, HIPAA/HITECH requires that we use or disclose or request from others only the minimum PHI necessary to accomplish the intended purpose of such use or disclosure. This concept is referred to as the "Minimum Necessary" rule.

The rules and regulations regarding the use and disclosure of PHI are complex. If you have any doubt as to whether PHI should be used or disclosed, consult with your manager.



What is an unauthorized use or disclosure of PHI?

An unauthorized use or disclosure occurs when "unsecured" PHI is sent to or accessed by someone who did not have the right to see it. Generally, "unsecured" means that the PHI was not rendered unusable, unreadable or indecipherable to the unauthorized person who received it (e.g., the PHI was not encrypted). A "data breach" encompasses unauthorized use, disclosure or acquisition of PHI in a manner not permitted under the law, which comprises the security or privacy of PHI.

What can I do to safeguard against unauthorized uses or disclosures of PHI?

Follow Medical Mutual's policies and procedures regarding the use, disclosure and transmission of data that includes PHI.

What happens if an unauthorized use or disclosure occurs?

All employees are responsible for documenting and reporting a suspected or actual exposure of customer private, sensitive or regulated data, paper or electronic, as soon as an exposure is known or suspected. This includes any unauthorized uses or disclosures of companies acting on our behalf, known as business associates. If you suspect that an unauthorized use or disclosure of PHI has occurred, report the issue immediately to your manager.

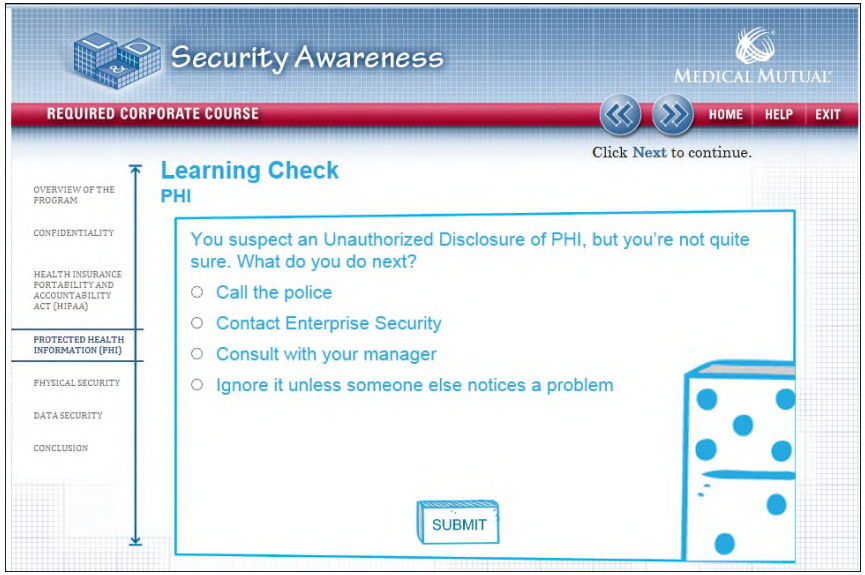
You and your manager are also required to complete a HIPAA Data Exposure Incident Form that can be found out on PartnerNet. In the event of a breach of unsecured protected health information, Medical Mutual must notify affected individuals, HHS and, in some cases, even the media.

Remember, all it takes is one small mistake, and everything can come crashing down.

What does "minimum necessary" mean when disclosing PHI?

Always consider what is requested and only provide the data that is absolutely needed for the intended purpose.
Always send data that includes PHI through "secured" means. Unless is it absolutely necessary, physical documents containing PHI should not be sent via U.S. mail, overnight courier, etc. The following policies explain the proper ways to transmit PHI:

Encryption,
De-Identified Information
Electronic Communications: E-Mail, IM, and Internet Usage.



Learning Check

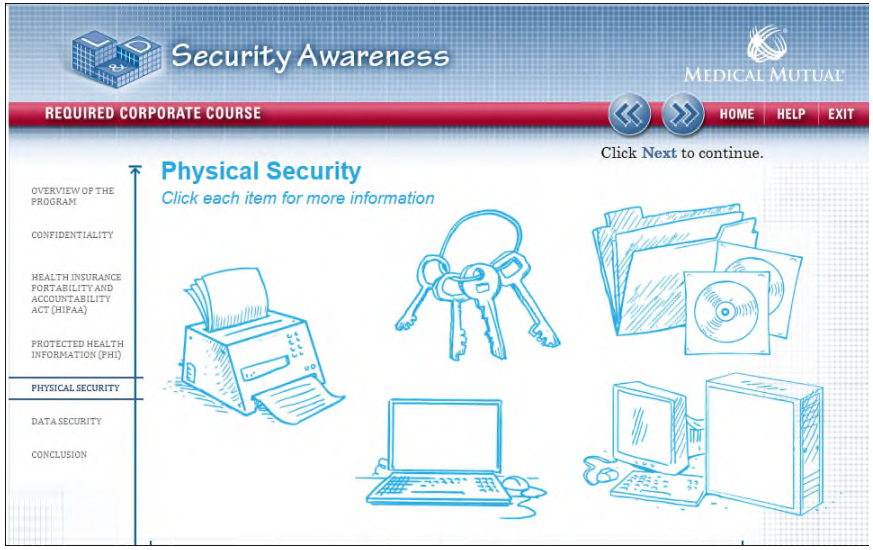
You suspect an Unauthorized Use or Disclosure of PHI, but you're not quite sure. What do you do next?

- **Call the police?** *Incorrect. You should consult with your manager. Together you can determine if there is a possibility of a breach and complete a Data Exposure Incident Form.*

- **Contact Enterprise Security?** *Incorrect. You should consult with your manager. Together you can determine if there is a possibility of a breach and complete a Data Exposure Incident Form*

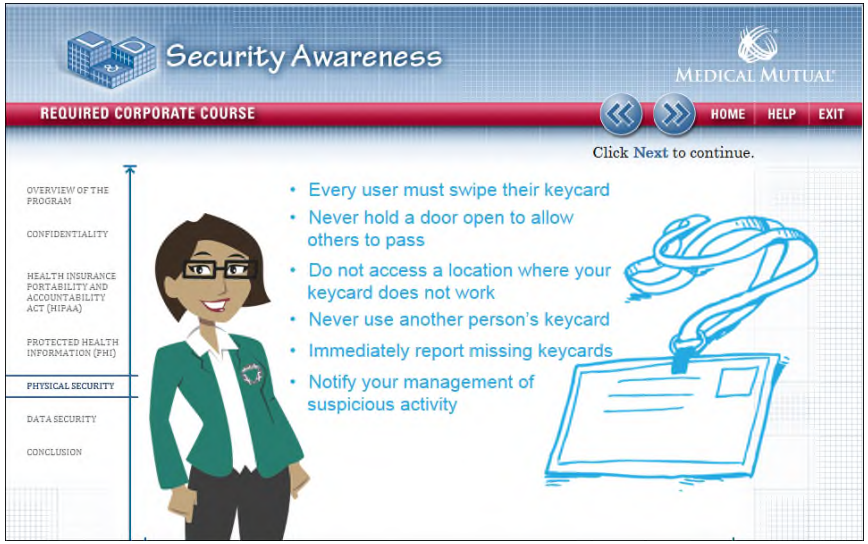
- **Consult with your manager?** *Correct! When in doubt always contact your manager. Together you can determine if there is a possibility of a breach and complete a Data Exposure Incident Form.*

- **Ignore it unless someone else notices a problem?** *Incorrect. You should consult with your manager. Together you can determine if there is a possibility of a breach and complete a Data Exposure Incident Form.*



Physical security controls exist to protect Medical Mutual resources and employees.

- Don't leave sensitive information at shared printers. Notify your supervisor if you find sensitive information at a printer for an extended period of time.
- Store office keys and access cards in a secure area.
- Keep paper files, CDs and DVDs containing sensitive information in locked drawers.
- Activate your password-protected screensaver on your computer when away from your work area.
- Back up data or store it on a server that is backed up frequently

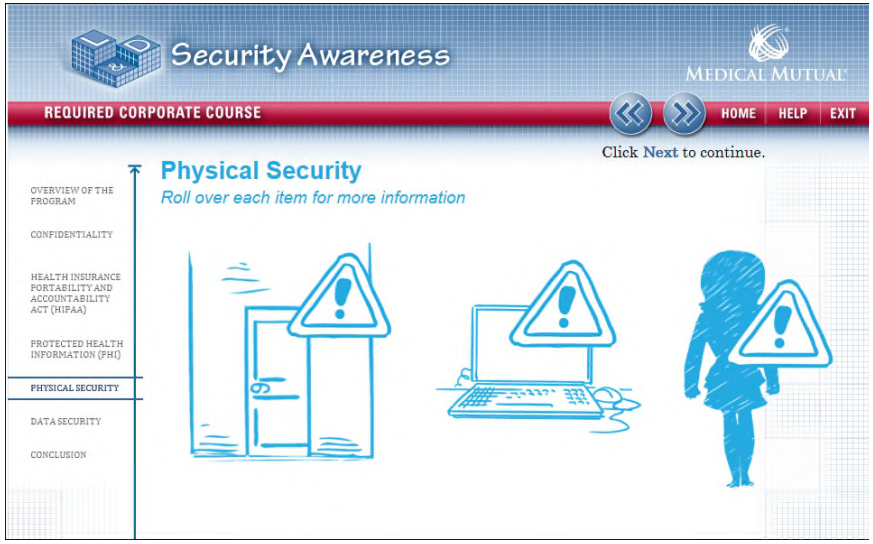


Keycards are assigned to all authorized staff as a means of ensuring the safety and security of all employees, MMO facilities, equipment and data.

Here are some reminders for the proper use of your keycard:

- Every user must swipe their keycard when accessing through a secure door
- Never hold a door open to allow others to pass
- Do not access a location where your keycard does not work
- Never use another person's keycard
- Immediately report missing keycards to the Medical Mutual Helpdesk and
- Notify your management of suspicious activity

You wouldn't allow a stranger to walk into your home, so why do it at work?

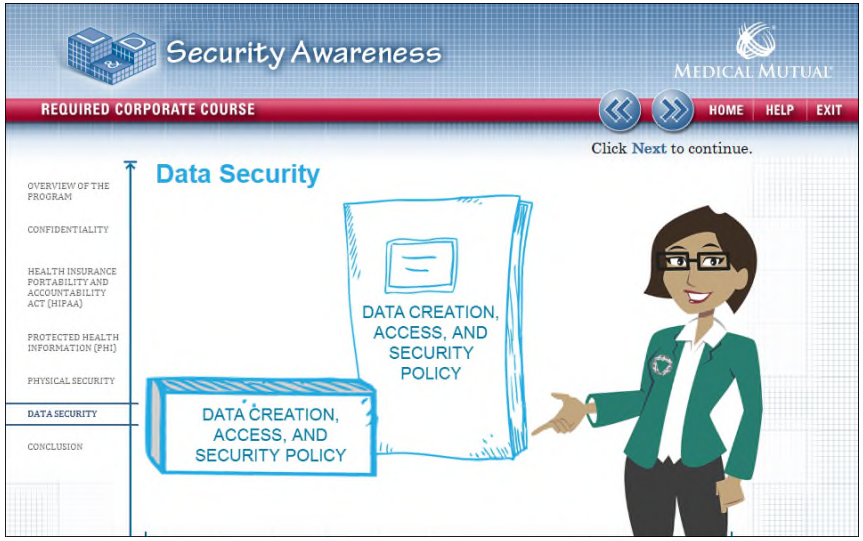


Roll over the caution signs shown here to learn how you can protect company information.

- Don't allow unauthorized building access or tailgating. Tailgating occurs when an authorized user accesses a door, and is followed by one or more people who may or may not be authorized to enter. When entering a secured area, ALL employees need to swipe their badges.

- When working remotely, you can put the information stored on the laptop and the network at risk. Always consider the internet security of public networks before connecting.

- Always pay close attention to your surroundings. Report any and all suspicious activity.



The Corporate Data Security Policy applies to all information created, accessed or used by Medical Mutual. It is designed to protect both the data and the Company should data misuse or loss occur. It is important to note that this information is the property of Medical Mutual. It should be disclosed only on a need-to-know basis. All employees share the responsibility of ensuring that work is performed in a secure environment by following secure practices at all times. If everyone takes responsibility, we will ensure that there are no weak links to leverage.

There are three questions you should ask yourself when determining the best way to communicate sensitive data.

1. What does the data show?
2. Where does it need to go?
3. How secure should it flow?

What does the data show?

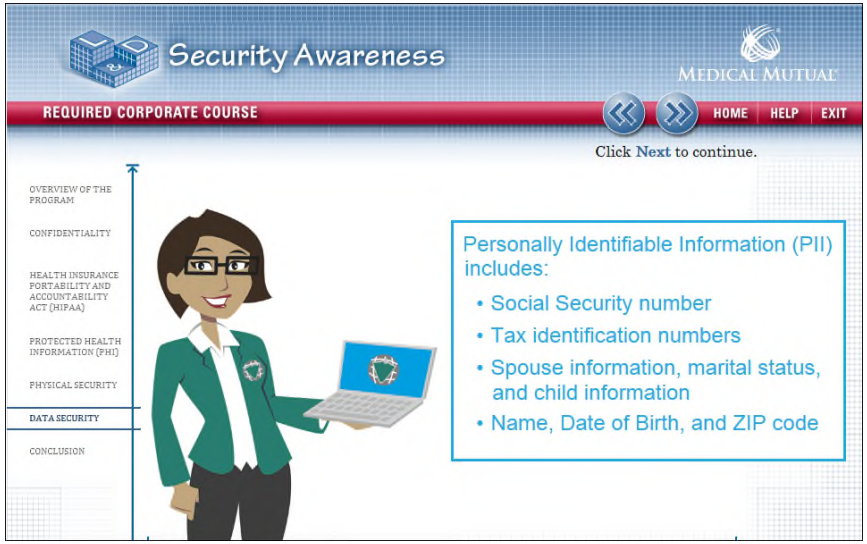
Identify whether your message or file includes sensitive data. If so, send ONLY the minimum necessary information required to accomplish the task at hand.

Where does it need to go?

Identify if the information is needed for internal or external purposes and how the data needs to be sent. Is the data being sent to members, providers, business partners, publications or to the media? Use the *Permissible Disclosures of Protected Health Information policy* to determine if the recipient should be receiving the data to begin with. When in doubt consult with your manager.

How secure should it flow?

Communicate sensitive data securely and according to Medical Mutual's data transmission protocol as specified in the Encryption Policy.

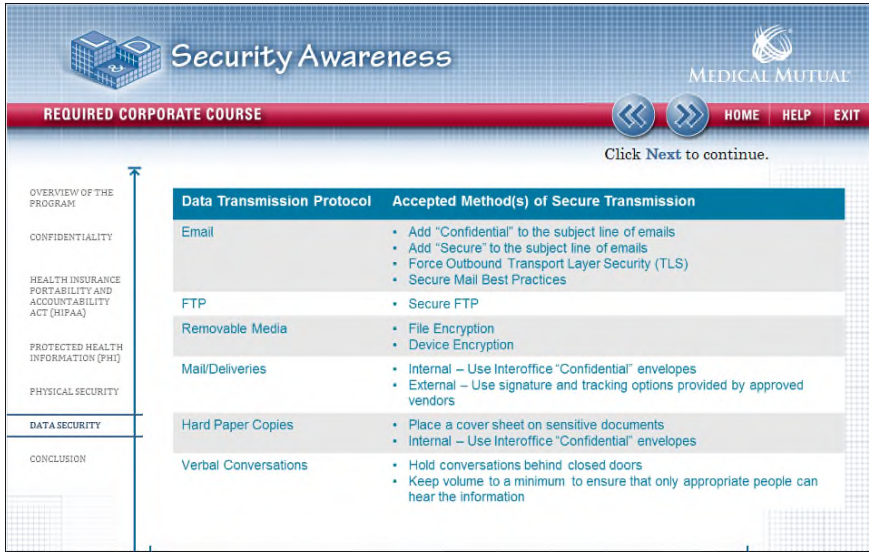


As you've already learned, PHI is considered sensitive data. Here are some additional data types that are considered to be sensitive.

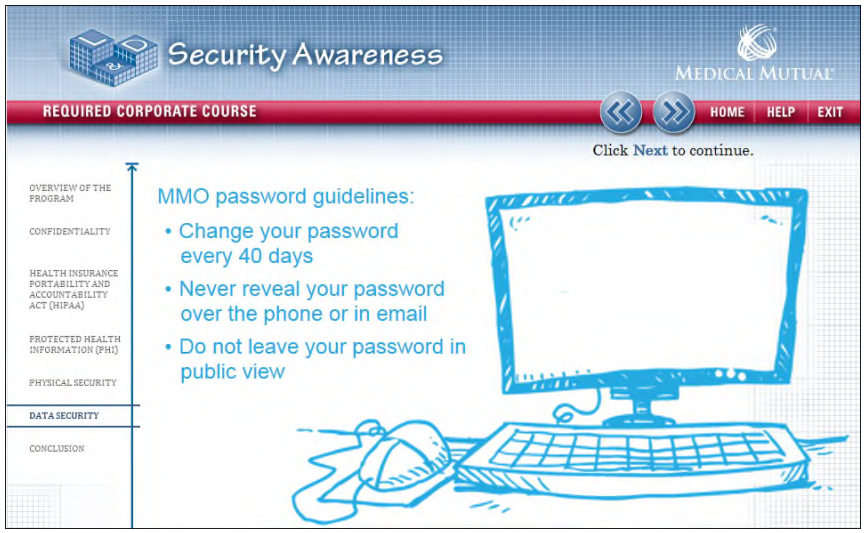
Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Examples of sensitive PII elements include but are not limited to:

- Social Security number, full and truncated
- Tax identification numbers
- Spouse information, marital status, child information and
- Name + DOB + Zip Code



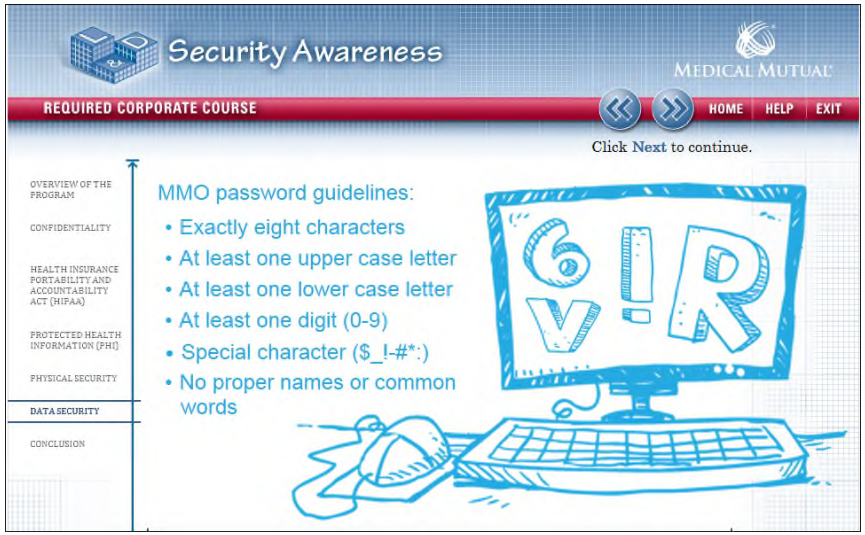
Depending on the type of data being sent, and to whom, you will need to identify the appropriate sensitive delivery protocol. Use this chart to help guide your decisions on how to send sensitive data internally and externally.



Each employee accesses the company network and various applications with a user name and password. Passwords must be protected. Do not share passwords with anyone who is not authorized to access data.

Here are some guidelines to help you select and maintain secure passwords:

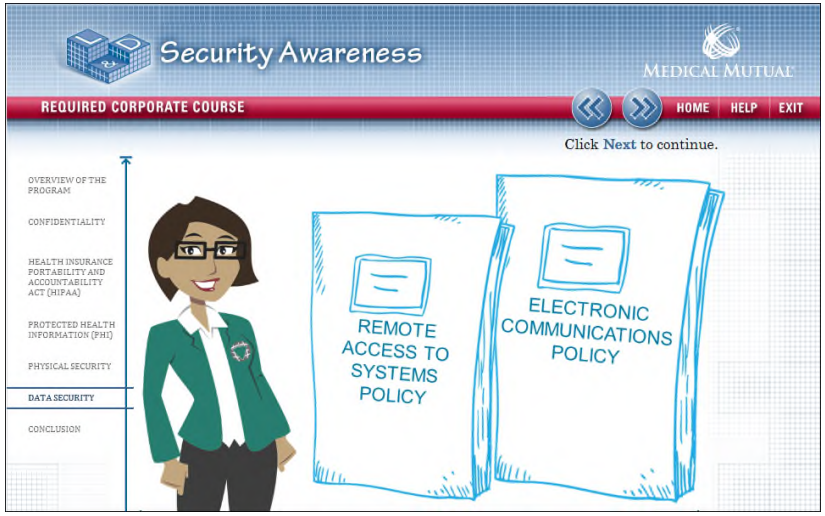
- Employees are required to change their LAN password every 40 days;
- Never give out a password over the phone or in email messages; and
- Do not leave your passwords in public view.



To maintain the highest level of protection, your passwords **MUST** meet the following MMO guidelines. They must:

- Be exactly eight characters in length;
- Contain at least one upper case letter;
- Contain at least one lower case letter;
- Contain at least one digit (0-9);
- Contain a special character ($_!-#*:); and

Not contain a proper name or a common word.



In this section, we'll review the Electronic Communications Policy and the Remote Access to Systems Policy. These policies apply to all electronic media and services that are:

- Accessed on or from Company premises
- Accessed using Company computer equipment or via Company-paid access methods and
- Used in a manner that identifies the individual with the Company

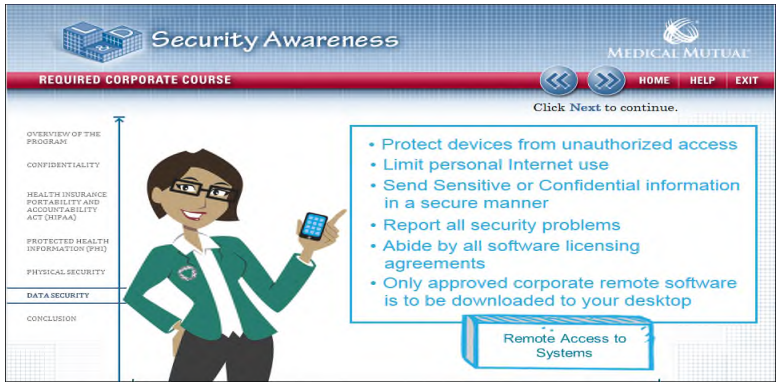
Employees are asked to show responsibility in regard to electronic media and services. This includes not using communications that are discriminatory or harassing, obscene or pornographic or threatening. While you are permitted some leeway for personal use, you should not abuse the privilege.

Don't use company resources for personal gain. For example, don't use company equipment to work on personal projects or let your family use it. And never remove confidential information from work or our secure network servers.

You must respect the confidentiality of others' communications. Therefore, you are prohibited from monitoring or intercepting files or electronic communications. Don't attempt to obtain access to systems or accounts you're not authorized to use. You also should never use another person's logins or passwords.

The Company reserves the right to review any employee's electronic files and messages at any time.

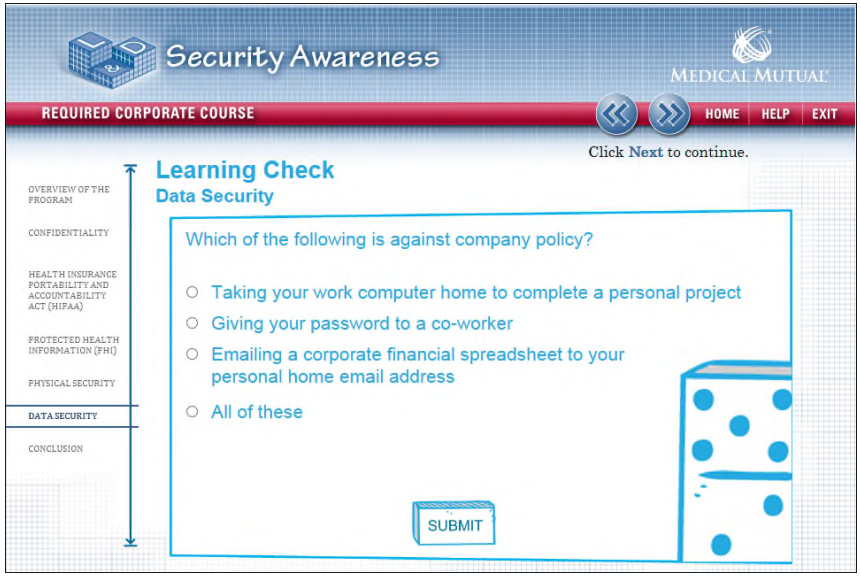
This ensures media and services are being used in compliance with the law and Company policy. This policy covers email, instant messaging and Internet usage.



The Internet is an important business tool. It allows employees to communicate with each other, customers, vendors and other associates.

Our Company has some security measures in place to protect our network. Some work to prevent sensitive data from leaving Medical Mutual's secured network in an unsecured format. Others work to detect and prevent the introduction of harmful malware. However, you must also do your part by following these rules:

- Protect all of your mobile devices, like laptops, tablets and cell phones from unauthorized access;
- Limit personal Internet use and ensure that it doesn't affect work priorities;
- Send Sensitive or Confidential information in a secure manner;
- Report all security problems or suspected violations to your management;
- Abide by all software licensing agreements, copyright laws and other applicable regulations; and
- Only approved corporate remote software is to be downloaded to your desktop.



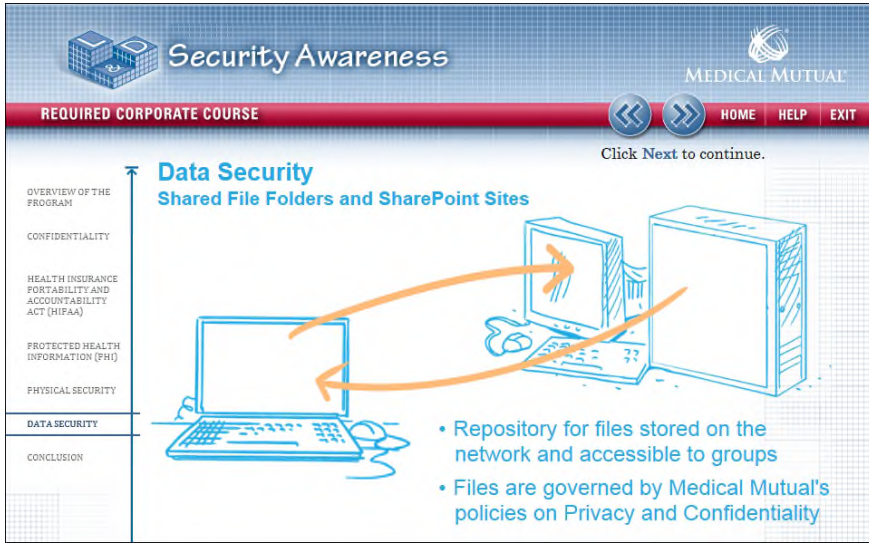
Don't be another weak link in the chain reaction. Answer this question correctly to proceed.

Which of the following is against corporate policy?

- Taking your work computer home to complete a personal project
- Giving your password to a co-worker
- Emailing a corporate financial spreadsheet to your personal home email address
- All of these

Correct answer = <u>All of these</u>

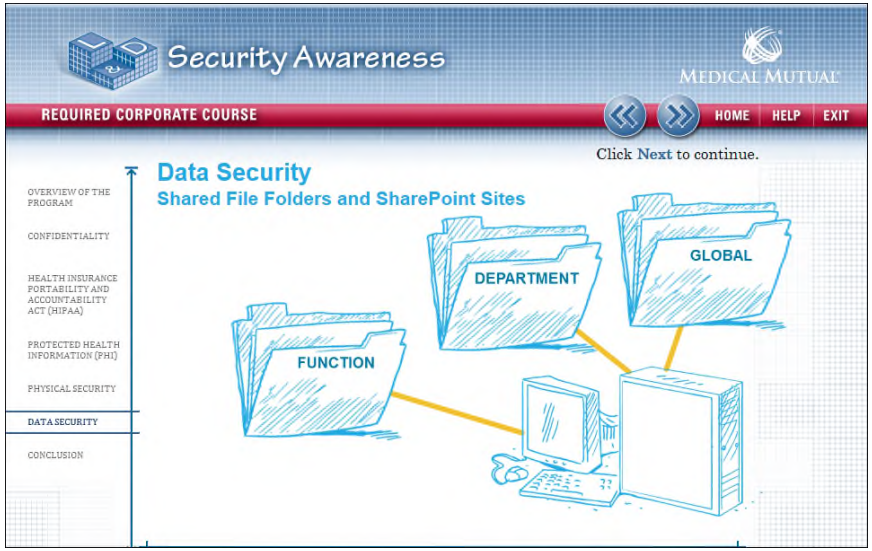
Each of these actions is in conflict with corporate policies.



Shared file folders, commonly referred to as the “S Drive” or “Department Drive”, as well as SharePoint sites play an important role in our business processes and productivity. They provide an organized, secure way of storing and sharing the information we use.

A shared folder is a repository for files that are stored on the company network and are accessible to groups of users. A key benefit of using the shared folders is that Medical Mutual backs up the data regularly to prevent important files from data loss.

Like all sensitive information, files placed into shared folders or SharePoint are governed by Medical Mutual’s policies on Privacy and Confidentiality, and must be carefully handled and protected from unauthorized access. This means understanding the types of shared folders and SharePoint sites and when it is appropriate to use them.

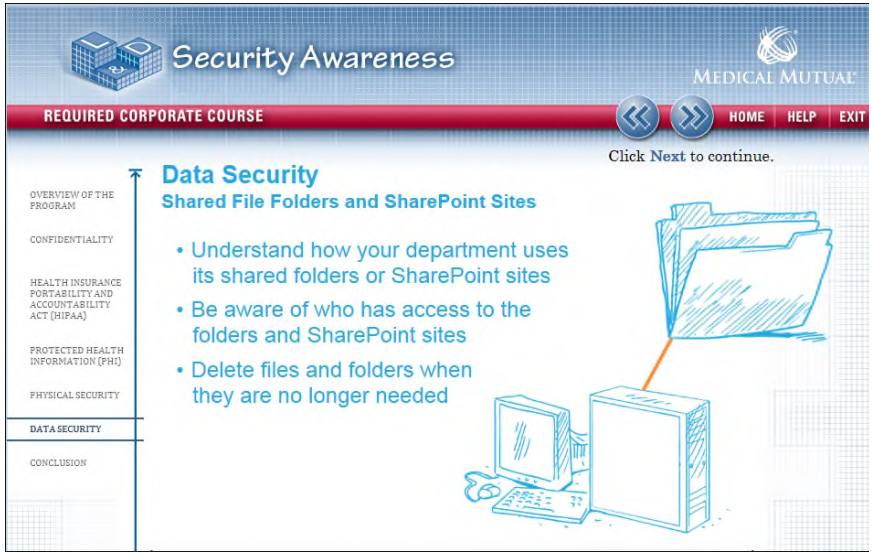


Some shared folders, like ones that contain the word GLOBAL, span many departments and allow a large number of employees to access the files and folders. When saving to this location, ask yourself, “Should all employees have access to this file?”

Access to folders can be restricted by department or function so that only employees in those departments or functions can read or update the files in that folder. Typically, a business department has at least one departmentally shared folder and that department is responsible for defining what types of information should be saved to that location.

Similarly, SharePoint sites can be accessible to a large number of employees across the organization or their access lists can be restricted by department or function.

Contact the Helpdesk if your work group requires a secure department only folder directory or SharePoint site.



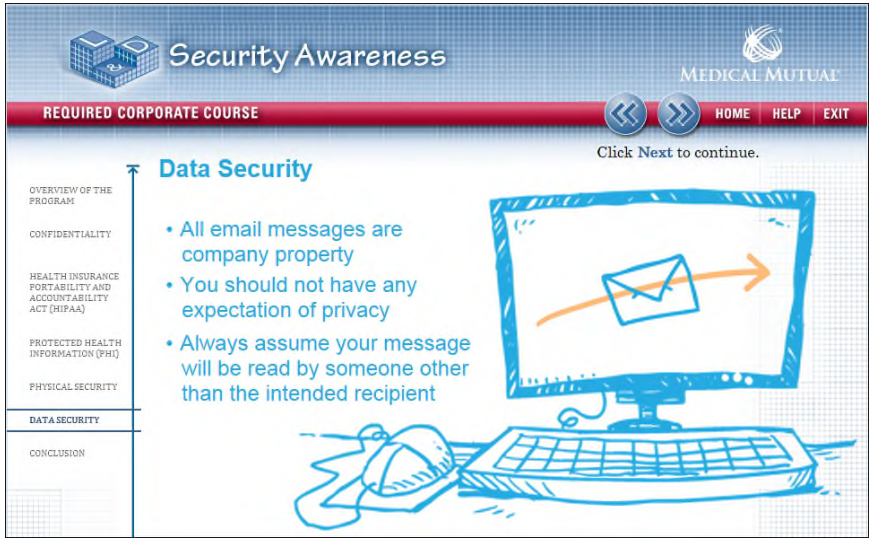
How can you make the best use of shared folders and SharePoint sites?

- Understand how your department uses its shared folders or SharePoint sites. If you are unsure or find a file that has been misplaced, notify your management;
- Be aware of who has access to the folders and SharePoint sites in which you save information. Restrict access to the correct subset of users; and
- Delete files and folders when they are no longer needed.

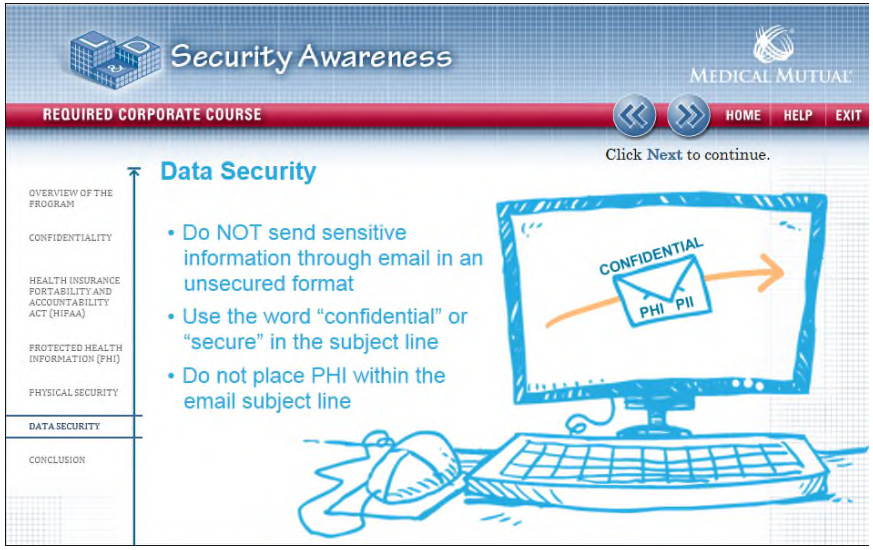
Match the document type to the correct file folder.

Correct answers are:

- NON SENSITIVE DATA FILE = GLOBAL folder
- BIRTHDAY EMAIL = PERSONAL folder
- DEPARTMENTAL MEMO = DEPARTMENT folder



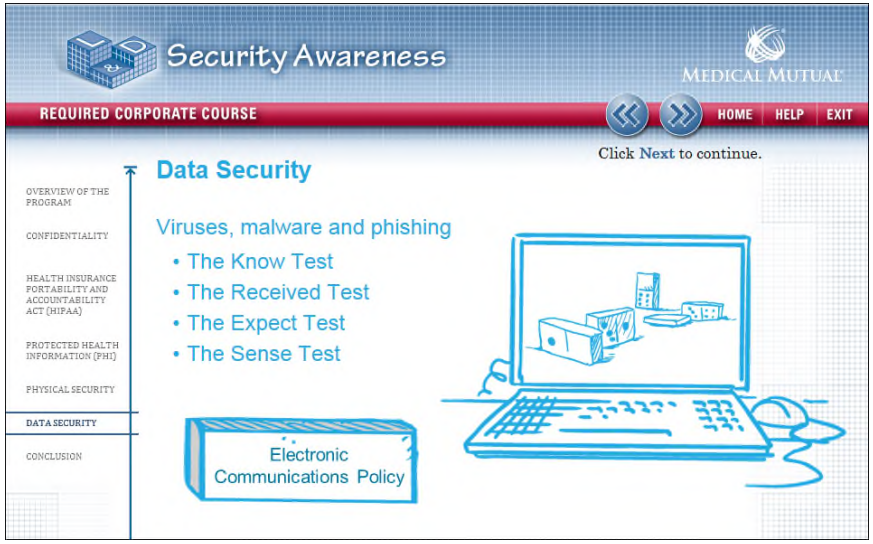
All email messages sent or received through the corporate email system are company property. You should not have any expectation of privacy with respect to these messages. Always assume your message will be read by someone other than the intended recipient.



Do NOT send sensitive information through email in an unsecured format. "Secure Messaging" is a means of transmitting sensitive information via corporate email to a recipient outside of the company. Always use Secure Messaging when you are sending corporate sensitive or personally identifiable information (PII) or protected health information (PHI) via email to an external recipient. Sending a secure email message requires the use of the word "confidential" or "secure" in the email subject line. The recipient of a Secure Messaging email has 30 days in which to visit a secured location to view the sent message. Always consider the "minimum necessary" principle when sending sensitive data via email.

To send a Secure Messaging email:

- Use the word "confidential" or "secure" in the subject line and
- Do not place PHI within the email subject line (for example: a SSN)



Did you know that a significant number of viruses, malware and phishing scams come through email? This is especially true for personal email, which can be accessed through the company Internet.

Email attacks are becoming more sophisticated, targeting attacks on companies and individuals. Many malicious emails are designed to look like official business, such as a bank requesting customer data.

For this reason, never open unsolicited emails or attachments. Never follow email instructions that require you to complete a computer task, click a link or provide information unless it is from an authorized source in Medical Mutual Technical Support or Enterprise Security.

You can ensure safe email usage by opening only those emails that pass all of these tests:

- *The Know Test:* Is the email from someone you know?
- *The Received Test*: Have you received email from this sender before?
- *The Expect Test:* Were you expecting email with an attachment from this sender?
- *The Sense Test:* Is there a message subject? Does the email content and attachment make sense in relation to the subject line and the name of the attachment?

If you suspect an email is a phishing attempt, please contact the Medical Mutual Helpdesk to discuss.

Social media outlets such as Facebook, Twitter and LinkedIn have grown in popularity and are quickly becoming a standard form of communication. Medical Mutual expects that employees will use common sense when using social media. This means that an employee is expected not to take any actions on social media that may harm others, the Company, its employees, members, customers and business partners. Some guidelines to follow are:

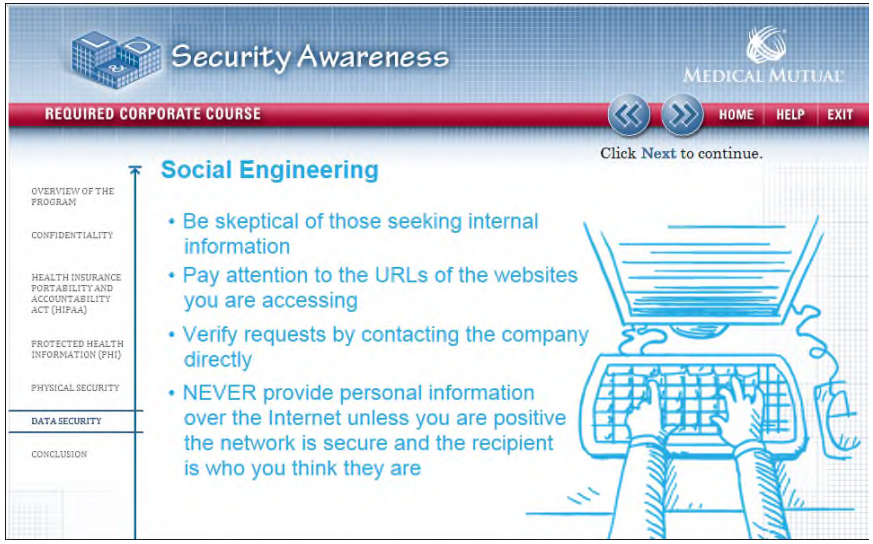
- Work time should be devoted to the business of Medical Mutual; social media should not interfere with work commitments; and
- If an employee does use social media they must comply with Medical Mutual policies.

Any employee using social media for personal reasons should keep in mind that the information could be viewed by anyone with an Internet connection, including Medical Mutual customers, co-workers, members of management, competitors, members of the media and the general public. Therefore, employees are prohibited to post or share any information about Medical Mutual, use the Company logo or release PHI.

If an employee accesses social media on Company computers, handheld devices or systems, they must not assume that their usage is private and that the Company will not review all usage. Remember that you are a representative of Medical Mutual and what you say directly reflects our organization.

Social engineering is a type of attack that relies on human interaction and often involves deceiving people to circumvent the regular security procedures of a company. An attacker will try to obtain information by posing as a person of authority, especially within an organization/enterprise. Common examples include an attacker posing as a member of the helpdesk and asking for your LAN password over the phone or an official looking email requesting personal information like a SSN.

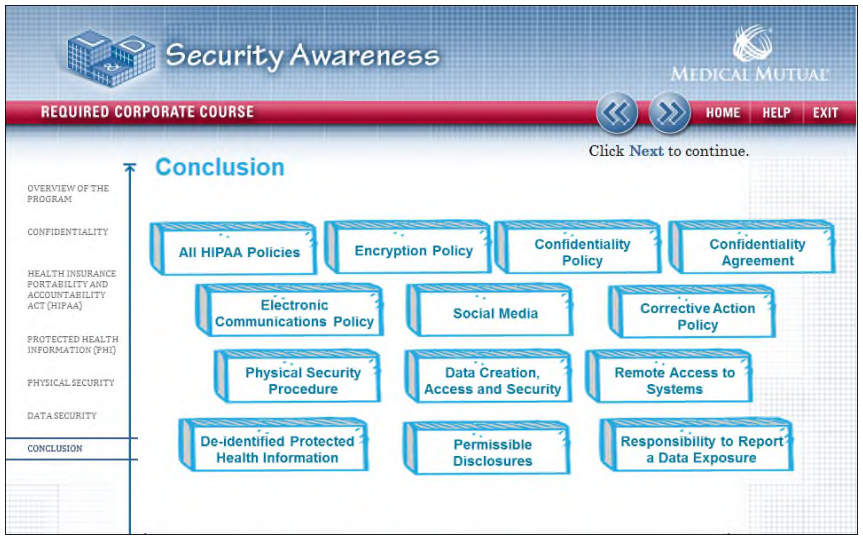
Although we all want to be helpful employees, it is important to always adhere to Corporate Policy when sharing information.



There are several ways you can avoid becoming a victim of social engineering:

- Always be skeptical of those seeking internal information about you or the Company;
- Be suspicious of spontaneous phone calls/visits/emails from people asking about internal information, including employee phone numbers;
- Pay attention to the URLs of the websites you are accessing. Malicious websites may look similar to valid sites with slight variations, such as .net versus .com;
- If you are unsure if a request is legitimate, try to verify it by contacting the company directly; and
- NEVER provide personal information over the Internet unless you are absolutely positive your network is secure and the recipient is who you think they are.

If you have concerns about suspicious activity, contact your manager and Enterprise Security, and they will determine which steps to take next.



As technology improves, Medical Mutual works to continually improve its security. However, YOU are the first line of defense. Preventing issues altogether or addressing issues quickly can play a large role in avoiding the domino effect.

This module is only a basic overview of the various policies and procedures put in place to secure our data, premises and employees. If you have not reviewed all the necessary policies, please take the time to do so.